National Infrastructure Protection Center
CyberNotes

Issue #2002-03 *February 11, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between January 21 and February 7, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
AHG[1]	Multiple	HTML search 1.0	A vulnerability exists because user input is not properly sanitized in the 'search.cgi' script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	HTML 'Search.CGI' Arbitrary Command	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Apache Group[2]	Multiple	Apache 2.0.28 Beta	A vulnerability exists in 'php.exe,' which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Apache 'php.exe' Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[1] Securiteam, January 29, 2002.
[2] Bugtraq, February 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Caldera[3]	Unix	UnixWare 7.1.1	A vulnerability exists in the library functions that are used to manipulate message catalogs, which could let a malicious user obtain elevated privileges.	Patch available at: ftp://stage.caldera.com/pub/security/unixware/CSSA-2002-SCO.3/erg711179.Z	UnixWare Library Function	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Castelle[4]	Multiple	FaxPress Software 6.3	A vulnerability exists when a print job is submitted with an incorrect password, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FaxPress Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[5]	Unix	tac_plus F4.0.4 alpha	A vulnerability exists because accounting files are created insecurely, which could let a malicious user modify/remove accounting files.	No workaround or patch available at time of publishing.	Tac_Plus Insecure Accounting File	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems [6]	Windows NT 4.0/2000	Secure ACS for Windows NT 3.0.1	A vulnerability exists because users in the NDS (Novell Directory Services) database that have expired or disabled accounts may still authenticate with the service.	Patch available at: http://www.cisco.com/pcgi-bin/tablebuild.pl/cs-acs-win	Secure ACS NDS Expired/ Disabled User Authentication	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Compaq[7]	Unix	Tru64 4.0d	A Denial of Service vulnerability exists when a scan is received across the network.	No workaround or patch available at time of publishing.	Tru64 Scan Denial Of Service	Low	Bug discussed in newsgroups and websites. This vulnerability can be exploited with a scanning tool.
Compaq[8]	Unix	Tru64 4.0g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f PK6 (BL17), 4.0f, 4.0d PK9 (BL17), 4.0d, 5.0a PK3 (BL17), 5.0 PK4 (BL17), 5.0, 5.1a, 5.1 PK4 (BL18), 5.1 PK3 (BL17), 5.1	A race condition vulnerability exists in the Unix kernel, which could let a malicious user obtain root access.	Patch available at: http://ftp1.support.compaq.com/public/unix/ You must have installed Tru64 UNIX 4.0G and PK3 (BL17) before applying the patch.	Tru64 Kernel Race Condition	**High**	Bug discussed in newsgroups and websites.

[3] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.3, February 7, 2002.
[4] Bugtraq, February 5, 2002.
[5] Bugtraq, January 30, 2002.
[6] Cisco Security Advisory, CI-02.02, February 7, 2002.
[7] Bugtraq, January 30, 2002.
[8] SecurityFocus, January 31, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Compaq[9]	Windows 98/ME/ 2000	Intel PRO/ Wireless 2011B LAN USB Device Driver 1.5.16.0, 1.5.18.0	A vulnerability exists because the WEP (Wired Equivalent Privacy) Key is stored in plaintext, which could let an unprivileged malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Intel PRO/Wireless 2011B LAN USB Device Driver Plaintext WEP	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
DC Scripts[10]	Unix	DCForum 5.0, 6.0, 6.21, 2000 1.0	A vulnerability exists because predictable passwords are generated, which could let a remote malicious user obtain elevated privileges.	Upgrade available at: http://www.dcscripts.com/FAQ/retrieve_password.txt	DCForum Predictable Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
DeleGate[11]	Windows NT 4.0/2000, Unix	DeleGate 7.7.0, 7.7.1, 7.8.0, 7.8.1	Multiple buffer overflow vulnerabilities exist in various proxy components, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	DeleGate Multiple Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Eshare Communi-cations Incorpor-ated[12]	Windows NT 4.0/2000	Eshare Expressions 1.0, 2.0	A Directory Traversal vulnerability exists due to insufficient string validation, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Eshare Expressions Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Etype[13]	Windows 95/98/NT 4.0/2000, XP	Eserv 2.97	Two vulnerabilities exist: a Denial of Service vulnerability exists when a large number of 'PASV' requests are sent to the server; and a vulnerability exists which could let a remote malicious user connect to an arbitrary port via the 'PORT' command.	Upgrade available at: ftp://ftp.eserv.ru/pub/beta/2.98/Eserv3123.zip	EServ Multiple Vulnerabilities	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
FAQ-O-Matic[14]	Unix	FAQ-O-Matic 2.711, 2.712	A cross-site scripting vulnerability exists because script code is not properly filtered from URL parameters, which could let a remote malicious user execute arbitrary code.	Patch available at: http://sourceforge.net/cvs/?group_id=10674	Faq-O-Matic Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
FreeBSD[15]	Unix	FreeBSD 4.1, 4.1.1, 4.2-4.5	A Denial of Service vulnerability exists due to a race condition in the FStatFS Syscall.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:09/fstatfs.patch	FreeBSD FStatFS Syscall Race Condition	Low	Bug discussed in newsgroups and websites.

[9] Bugtraq, January 28, 2002.
[10] DCScripts Security Advisory, January 31, 2002.
[11] Global InterSec LLC Advisory, 2002012101, February 7, 2002.
[12] Bugtraq, February 5, 2002.
[13] Bugtraq, January 29, 2002.
[14] Superpetz Advisory #002, February 4, 2002.
[15] FreeBSD Security Advisory, FreeBSD-SA-02:09, February 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hanterm[16]	Unix	Hanterm 3.3	A buffer overflow vulnerability exists when a maliciously constructed parameter is sent to the server, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Hanterm Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Hosting Controller[17]	Windows NT 4.0/2000	Hosting Controller 1.1, 1.3, 1.4b, 1.4, 1.4.1	A vulnerability exists when an invalid username is entered, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Hosting Controller Invalid Username	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Infopop[18]	Windows NT 4.0/2000, Unix	UBBThreads 5.4; Wired Community Software WWW Threads 5.0.9, 5.0.8, 5.0.6, 5.0	A vulnerability exists when a second file extension is added because only the first file extension is checked, which could let a remote malicious user upload arbitrary files.	Upgrade available at: http://www.infopop.com/support/ubbthreads/index.html	UBBThreads/ WWWThreads Arbitrary File	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Internet Security Systems[19]	Windows 2000, XP	BlackIce Agent 3.0, 3.1, BlackICE Defender 2.9caq, 2.9cap; RealSecure Server Sensor 6.0.1 Win, 6.5 Win	A remote Denial of Service vulnerability exists when a continuous series of ICMP Echo Request 10,000 byte packets are sent to the server.	Workarounds available at: http://www.iss.net/security_center/alerts/advise109.php	BlackICE and RealSecure Denial of Service	Low/**High** **(High if DDoS best practices not in place.)**	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Jelsoft Enterprises[20]	Multiple	vBulletin 2.2.0	A cross-site scripting vulnerability exists because user input is not properly sanitized, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	vBulletin Board Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[16] Bugtraq, February 7, 2002.
[17] ALPER Research Labs Security Advisory, ARL02-A01, January 26, 2002.
[18] Securiteam, February 3, 2002.
[19] Internet Security Systems Security Alert, ISS-109, February 4, 2002.
[20] Bugtraq, January 31, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Khaled Mardam-Bey[21]	Windows 95/98/ME/ NT 4.0/2000, XP	mIRC 2.1a, 2.3a, 2.4, 2.4a, 2.5a, 2.7a, 2.8c, 3.1-3.9, 4.0, 4.1, 4.5-4.7, 5.0, 5.1, 5.3-5.91	Two vulnerabilities exists: a buffer overflow vulnerability exists when a nickname over 200 characters long is used, which could let a remote malicious user execute arbitrary code; and a vulnerability exists which could let a remote malicious user direct mIRC users to a compromised IRC server by way of HTML code on a Web page.	Upgrade available at: http://www.mirc.com/get.html	MIRC Nickname Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
KICQ[22]	Unix	KICQ 2.0.0b1	A remote Denial of Service vulnerability exists when random characters are sent to the port.	No workaround or patch available at time of publishing.	KICQ Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
LICQ[23]	Unix	LICQ 1.0-1.0.4	A Denial of Service vulnerability exists when excessively long requests containing format strings are sent to the client.	The vendor has confirmed this issue and an upgrade is available via CVS.	LICQ Format String Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Lotus[24]	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Domino 4.6.1, 4.6.3, 4.6.4, 5.0, 5.0.1-5.0.9	Two Denial of Service vulnerabilities exist because URL requests for MS-DOS devices are not handled correctly and when a request for a DOS device from the CGI-BIN has an extension of 220 characters and is submitted approximately 400 times.	Upgrade available at: http://notes.net/qmrdown.nsf	Domino DOS Request Denial Of Service	Low	Bug discussed in newsgroups and websites. The URL request vulnerability can be exploited via a web browser and there is no exploit code required for the CGI-BIN vulnerability.
Lotus[25]	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Domino 5.0. 5.0.1-5.0.9	A vulnerability exists if a malformed URL is created because database files are not protected with a password, which could let a remote malicious user bypass authentication.	**Workaround:** Set the ACLs on the Web Administrator template to prevent anonymous access.	Domino Remote Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[21] Securiteam, February 3, 2002.
[22] Securiteam, February 3, 2002.
[23] Bugtraq, February 6, 2002.
[24] KPMG-2002004, February 4, 2002.
[25] Securiteam, February 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[26]	MacOS X 10.0-10.1.2	Office v. X	A Denial of Service vulnerability exists when certain types of malformed announcements are sent to the PID Checker service.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-002.asp	Office v. X for Macintosh PID Checker Denial of Service CVE Name: CAN-2002-0021	Low	Bug discussed in newsgroups and websites.
Microsoft[27]	Windows 2000	Exchange Server 2000, 2000SP1&2	A vulnerability exists in the way the System Attendant makes Registry configuration changes, which could let a remote malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-003.asp	Exchange Inappropriate Registry Permissions CVE Name: CAN-2002-0049	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[28]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, 2000 Advanced Server SP2SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2, 2000 Server Japanese Edition, 4.0, 4.0 alpha, 4.0 SP1-5, 4.0 SP1-5 alpha, XP, XP Home, XP Professional	A vulnerability exists because NTFS could allow files to be hidden, which could allow viruses to remain undetected on filesystems.	No workaround or patch available at time of publishing.	Windows NTFS File Hiding	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[26] Microsoft Security Bulletin, MS02-002, February 6, 2002.
[27] Microsoft Security Bulletin, MS02-003, February 7, 2002.
[28] SecurityFocus, January 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[29]	Windows NT 4.0/2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Server, 2000 Server SP1&2, NT Enterprise Server 4.0, NT Enterprise Server 4.0 SP1-6a, NT Server 4.0, NT Server 4.0 SP1-6a	A vulnerability exists when a trust relationship exists between two domains, the trusting domain will accept the list of Security Identifiers (SIDs) specified within authorization data, which could let a malicious user obtain elevated privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-001.asp	Windows Trusted Domain Membership CVE Name: CAN-2002-0018	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[30]	Windows NT 4.0/2000	IIS 5.0, SQL Server 6.5, 7.0, 7.0 SP1-3, 7.0SP1-3 alpha, 2000, 2000 SP1-2, 2000 Advanced Server, 2000 Advanced Server SP1-2, 2000 Datacenter Server, 2000 Datacenter Server SP1-2, 2000 Professional, 2000 Professional SP1-2, 2000 Server, 2000 Server SP1-2	A Denial of Service vulnerability exists in the Microsoft Distributed Transaction Service Coordinator (MSDTC) when a malicious user sends 1024 bytes of data to the listening port.	No workaround or patch available at time of publishing.	Microsoft MSDTC Service Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[29] Microsoft Security Bulletin, MS02-001, January 30, 2002.
[30] Bugtraq, January 31, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[31]	Windows NT 4.0/2000	Interix 2.2; Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 ServerSP1&2, 2000 Terminal Services, 2000 Terminal Services SP1&2	A buffer overflow vulnerability exists due to unchecked buffers in the code that handles the processing of Telnet protocol options, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-004.asp	Telnet Server Unchecked Buffer CVE Name: CAN-2002-00020	**High**	Bug discussed in newsgroups and websites.

[31] Microsoft Security Bulletin, MS02-004, February 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[32]	Windows NT 4.0	Site Server 3.0 with SP3 & prior, Commerce Edition 3.0 SP4 & prior	Multiple vulnerabilities exist: multiple cross-site scripting vulnerabilities exist, which could let a malicious user execute arbitrary code; a Denial of Service vulnerability exists when a TargetURL parameter is uploaded with more than 250 characters; multiple vulnerabilities exist in various administrative pages in the /SiteServer/Admin/ directory which could let an unprivileged malicious user obtain sensitive information; a vulnerability exists because LDAP passwords are stored in plaintext, which could let an unauthorized remote malicious user obtain sensitive information; a vulnerability exists due to the way the random LDAP_ Anonymous password is generated, which could let a malicious user obtain sensitive information; and a vulnerability exists in the web applications because user input is not properly validated before it is passed to an SQL query, which could let a malicious user insert arbitrary SQL commands.	No workaround or patch available at time of publishing.	Site Server Multiple Vulnerabilities	Low/ Medium/ **High** **(Medium if sensitive informa-tion can be accessed and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploits have been published for the cross-site scripting vulnerabilities. There is no exploit code required for the information disclosure vulnerabilities in the administrative pages and the LDAP_Anony-mous password generation vulnerability. Vulnerability has appeared in the press and other public media.
Microsoft[33]	Windows 95/98/ME/ NT 4.0/2000, XP	MSN Messenger Service 4.5, 4.6	A vulnerability exists because sensitive information can be obtained through an ActiveX control that is available to JavaScript programs.	No workaround or patch available at time of publishing.	MSN ActiveX Sensitive Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Mirabilis[34]	MacOS X 10.0-10.0.4 10.1-10.1.2	ICQ For MacOS X 2.6X Beta	A Denial of Service vulnerability exists when an excessively long request is sent to ICQ clients.	No workaround or patch available at time of publishing.	ICQ For MacOS X Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
MRTG[35]	Windows NT 4.0/2000, Unix	Multi Router Traffic Grapher CGI 2.9.17-win32, 2.9.17-unix	A vulnerability exists if a web request is submitted that contains unexpected arguments for script variables, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MRTG CGI File Display	Medium	Bug discussed in newsgroups and websites.

[32] RFP2201 Advisory, January 31, 2002.
[33] Bugtraq, February 2, 2002.
[34] Bugtraq, February 5, 2002.
[35] UkR Security Team Advisory, February 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MRTG Configuration Generator[36]	Multiple	MRTG config 0.5.9	Two vulnerabilities exist: a vulnerability exists in 'mrtg.cgi' which could let a malicious user obtain sensitive information; and a vulnerability exists if a HTTP request is submitted that contains unusual characters, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MRTG Path Disclosure Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[37, 38, 39, 40, 41, 42, 43, 44]	Unix	rsync 2.3.1, 2.3.2-1.2 sparc & PPC, 2.3.2-1.2 m68k, intel, ARM & alpha, 2.3.2, 2.4.1, 2.4.3, 2.4.4, 2.4.6,	Several vulnerabilities exist concerning the use of signed and unsigned variables, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://rsync.samba.org/rsync/download.html **SuSE:** ftp://ftp.suse.com/pub/suse/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Engarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **Debian:** http://security.debian.org/dists/stable/updates/main/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Trustix:** http://www.trustix.net/pub/Trustix/updates/ **RedHat:** ftp://updates.redhat.com/	rsync Signed Variable CVE Name: CAN-2002-0048	**High**	Bug discussed in newsgroups and websites.
Netgear[45]	Multiple	RT314/RT311 Gateway Router Firmware 3.22, 3.24, 3.25	A cross-site scripting vulnerability exists in the web interface for the router, which could let a malicious user execute arbitrary script and possibly obtain unauthorized administrative access.	No workaround or patch available at time of publishing.	RT314/RT311 Gateway Router Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
NetScreen Technologies[46]	Windows 95/98/ME/ NT 4.0/2000	ScreenOS 3.0.0-3.0.0r3, 2.6.1-2.6.1r4, 2.7.1-2.7.1r2	A Denial of Service vulnerability exists in the optional feature, IP Spoof protection.	Patch available at: http://www.netscreen.com/support/updates.html	ScreenOS IP Spoof Protection Denial of Service	Low	Bug discussed in newsgroups and websites.

[36] Bugtraq, February 4, 2002.
[37] SuSE Security Announcement, SuSE-SA:2002:004, January 25, 2002.
[38] Conectiva Linux Security Announcement, CLA-2002:458, January 25, 2002.
[39] EnGarde Secure Linux Security Advisory, ESA-20020125-004, January 25, 2002.
[40] Debian Security Advisory, DSA-106-1, January 26, 2002.
[41] Mandrake Linux Security Update Advisory, MDKSA-2002:009, January 28, 2002.
[42] Trustix Secure Linux Security Advisory, 2002-0025, January 28, 2002.
[43] Red Hat Security Advisory, RHSA-2002:018-10, January 30, 2002.
[44] Hewlett-Packard Company Security Advisory, HPSBTL0201-022, January 30, 2002.
[45] Bugtraq, February 3, 2002.
[46] NetScreen Security Advisory, January 21, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Network Associates [47]	Windows 95/98/ME/ NT 4.0/2000	PGP Security PGPfire 7.1	A vulnerability exists because the TCP/IP stack of the operating system is altered during installation, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PGPFire TCP/IP Alteration	Medium	Bug discussed in newsgroups and websites.
Nortel Networks[48]	Unix	WebOS 9.0	A vulnerability exists when a client has half-closed a session, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebOS Half-Closed Session	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Novell[49]	Windows NT 4.0	NetWare 5.0, 5.0SP5, 5.1	A vulnerability exists because access can be obtained to NT domain machines using a null password, which could let an unprivileged malicious user obtain Domain Admin access.	No workaround or patch available at time of publishing.	NetWare Null Password	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Oracle Corpora-tion[50]	Multiple	Oracle9i 9.0, 9.0.1, Oracle9iAS Web Cache 2.0.0.0-2.0.0.3	A vulnerability exists because source code is contained in .java files, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Oracle 9IAS .java Source Code	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Oracle Corpora-tion[51]	Windows NT 4.0/2000, Unix	Oracle9i 9.0, 9.0.1, Oracle9iAS Web Cache 2.00.3, 2.0.0.3, 2.0.0.2 NT, 2.0.0.2, 2.0.0.1, 2.0.0.0	Multiple vulnerabilities exist: a Denial of Service vulnerability exists when a request is made to the 'pls' module with an HTTP client Authorization header set but with no auth type; and multiple buffer overflow vulnerabilities exist in the PL/SQL Apache module, which could let a malicious user execute arbitrary code.	Patch available at: http://metalink.oracle.com	Oracle 9iAS Denial of Service and Buffer Overflow Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[47] Bugtraq, January 25, 2002.
[48] Securiteam, January 29, 2002.
[49] Bugtraq, January 31, 2002.
[50] NGSSoftware Insight Security Research Advisory, NISR06022002C, February 6, 2002.
[51] NGSSoftware Insight Security Research Advisory, NISR06022002B, February 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[52]	Multiple	Oracle database server 8.1.7.0.0, Oracle 8i Enterprise Edition 8.0.5.0.0, 8.0.6.0.1, 8.0.6.0.0, 8.1.5.1.0, 8.1.5.0.2, 8.1.5.0.0, 8.1.6.1.0, 8.1.6.0.0, 8.1.7.1.0, 8.1.7.0.0, Oracle8 8.0.3, 8.0.4, 8.0.5.1, 8.0.5, 8.0.6, 8.1.5-8.1.7, 8.0.1, 8.0.2, 8.0.4-8.0.6, 8.1.5-8.1.7.1 9.0, 9.0.1	A vulnerability exists because there is no authentication required for the listener process, which could let a remote malicious user execute arbitrary functions.	No workaround or patch available at time of publishing.	Oracle TNS Listener Arbitrary Function	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP[53]	Multiple	PHP 3.0-3.0.13, 3.0.16, 4.0, 4.0.1pl2, 4.0.1, 4.0.3-4.0.6, 4.1, 4.1.1	A vulnerability exists because the MySQL client library does not perform proper checking on 'LOAD DATA INFILE LOCAL' statements, which could let a malicious user bypass restrictions to gain unauthorized access to restricted filesystems.	No workaround or patch available at time of publishing.	PHP MySQL Safe_Mode Filesystem Circumvention	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
PhpSms Send[54]	Multiple	PhpSmsSend 1.0	A vulnerability exists because user input is not properly validated, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	PhpSmsSend Remote Arbitrary Command	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
PhpWeb Things[55]	Multiple	PhpWeb Things 0.4	A vulnerability exists in the 'core/main.php' helper script, which could let a remote malicious user modify database queries.	Upgrade available at: http://freshmeat.net/redir/phpwebthings/15746/url_zip/phpwebthings-0.4.1.zip	PHPWeb 'core/main.php' Script	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[52] NGSSoftware Insight Security Research Advisory, NISR06022002A, February 6, 2002.
[53] Security Advisory, DW020203-PHP, February 3, 2002.
[54] Bugtraq, January 29, 2002.
[55] SecurityFocus, February 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Portix-PHP[56]	Unix	Portix-PHP 0.4.02, 0.4.0	A vulnerability exists because non-expiring cookies are used for session management, which could let a malicious user obtain administrative access.	No workaround or patch available at time of publishing.	Portix-PHP Cookie Manipulation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Portix-PHP[57]	Unix	Portix-PHP 0.4.02, 0.4.0	Two Directory Traversal vulnerabilities exist because web requests are not properly filtered in the 'view.php'and 'portix-php' scripts, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Portix-PHP 'view.php' and 'index.php' Directory Traversal Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SAP[58]	Windows 95/98/NT 4.0/2000	SAPgui 4.6 for Windows, 4.6A-4.6D for Windows	A remote Denial of Service vulnerability exists due to the way invalid connections are handled.	No workaround or patch available at time of publishing.	SAPgui Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
SAS Institute, Incorporated[59] ***Corrected URL for Patch***	**Windows, OS/390, OS/2, Unix**	**SAS Base 8.0, 8.1**	**A buffer overflow and format string vulnerability exists in 'sastcpd,' which could let a malicious user execute arbitrary code with administrative privileges.**	**Patch available at: http://ftp.sas.com/techsup/download/hotfix/v81/base/81ba28/81ba28.html** ***(Note: The same hot fix can be applied to both releases.)***	**SASTCPD Buffer Overflow and Format String**	**High**	**Bug discussed in newsgroups and websites.**
SAS Institute, Incorporated[60]	Multiple	SAS Base 8.0, Integration Technologies 8.0	Two vulnerabilities exist: a vulnerability exists in 'sastcpd', which could let a malicious user execute arbitrary code as a root user; and a vulnerability exists in the 'netencralg' environment variable, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	'SASTCPD' and 'netencralg' Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
SGI[61]	Unix	IRIX 6.5.10m, 6.5.10f, 6.5.11, 6.5.11f, 6.5.11m, 6.5.12, 6.5.12f, 6.5.12m, 6.5.13, 6.5.13f, 6.5.13m, 6.5.14, 6.5.14f, 6.5.14m	A vulnerability exists when the 'vcp' Default Input is set to "Output Video," which could let a malicious user obtain sensitive information.	Vendor workaround available at: http://www.securityfocus.com/advisories/3836	IRIX Output Video Viewing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[56] SecurityFocus, February 6, 2002.
[57] SecurityFocus, February 6, 2002.
[58] Bugtraq, January 28, 2002.
[59] SN-004201, January 29, 2002.
[60] Bugtraq, January 30, 2002.
[61] SGI Security Advisory, 20020103-01-I, January 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sony[62]	Multiple	VAIO Manual for UAE, Southeast Asia, South Africa, Saudi Arabia, Oceania, East Asia, Manual Cyber Support for VAIO 3.0&3.1 Japan	A vulnerability exists in pre-installed software by exploiting particular software characteristics, which let a remote malicious user obtain unauthorized access through hidden programs in an Internet web page or E-mail message and take full control of the user's system. *Note: All VAIO personal computers from January 26th, 2002 are not susceptible to this issue.*	Sony has prepared a new program called the "VAIO Security Enhancement Program" and recommends that owners download and install the new software program immediately. For Customers who purchased VAIO outside Japan: http://www.css.ap.sony.com/Vaiofaq/security/agreementen.html For Customers who purchased VAIO in Japan: http://vcl.vaio.sony.co.jp/	VAIO Unauthorized Access	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Steve Kneizys[63]	Multiple	Agora.cgi 3.2-3.2r, 3.3a-3.3f, 3.3i, 3.3j, 4.0-4.0e	A vulnerability exists when a web request for a non-existent .html file is made, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Agora.CGI Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Micro-Systems, Incorpor-ated[64]	Unix	JRE (Linux Production Release) 1.2.2, 1.3.1	A Denial of Service vulnerability exists when a maliciously constructed java program is received.	No workaround or patch available at time of publishing.	JRE Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Tarantella, Incorpor-ated[65]	Unix	Enterprise 3 3.01, 3.0, 3.10, 3.11, 3.20	A race condition vulnerability exists during the installation process, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Enterprise 3 Race Condition	Medium	Bug discussed in newsgroups and websites.
Thunder-stone[66]	Multiple	Texis 3.0	A vulnerability exists when a HTTP request for an invalid path is submitted, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Texis Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Tolis Group[67]	Unix	BRU 17.0 Linux	A vulnerability exists due to the creation of insecure tmp files, which could let a malicious user overwrite system files, or obtain elevated privileges.	No workaround or patch available at time of publishing.	BRU Insecure Temporary File	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
wliang[68]	Unix	wmtv 0.6.5	Multiple buffer overflow vulnerabilities exist in the configuration file, which could let a malicious user execute arbitrary code.	Upgrade available at: http://security.debian.org/dists/stable/updates	WMTV Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites.

[62] Sony Security Announcement, January 25, 2002.
[63] Superpetz Advisory #001, January 28, 2002.
[64] SecurityFocus, January 30, 2002.
[65] Bugtraq, January 26, 2002.
[66] SecurityFocus, February 6, 2002.
[67] Bugtraq, January 26, 2002.
[68] Debian Security Advisory, DSA 108-1, February 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xinet[69]	MacOS, Unix	K-AShare 11.01 IRIX	A vulnerability exists because the default installation installs an icon directory with insecure permissions, which could let a malicious user obtain sensitive information.	Bug discussed in newsgroups and websites. There is no exploit code required.	K-AShare Insecure Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Xoops[70]	Unix	Xoops 1.0 RC1	A vulnerability exists because user input is not properly sanitized in the 'userinfo.php' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Xoops SQL 'userinfo.php' Sensitive Information	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Xoops[71]	Unix	Xoops 1.0 RC1	A cross-site scripting vulnerability exists in the 'pmlite.php' script and in the title field because script code is not sufficiently filtered, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Xoops Private Message Box Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between January 24 and February 7, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 16 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

[69] Bugtraq, January 28, 2002.
[70] Bugtraq, January 29, 2002.
[71] Bugtraq, January 29, 2002.

Date of Script (Reverse Chronological Order)	Script name	Script Description
February 7, 2002	**Hanterm_exp.c**	**Script which exploits the Hanterm Buffer Overflow vulnerability.**
February 5, 2002	**Osxicq.c**	**Script which exploits the ICQ For MacOS X Denial Of Service vulnerability.**
February 4, 2002	Ethereal-0.9.1.tar.gz	A GTK+-based network protocol analyzer that lets you capture and interactively browse the contents of network frames.
February 4, 2002	Gps-0.9.0.tar.gz	An advanced port scanner and a firewall rule disclosure tool that uses IP & ARP spoofing, sniffing, stealth scanning, ARP poisoning, IP fragmentation, and other techniques to perform stealth and untrackable information collection.
February 4, 2002	Lcrzo-4.04-src.tgz	A toolbox for network administrators and network malicious users that contains over 200 functionalities using network library lcrzo.
February 3, 2002	Mircexploit-v591.c	Script which exploits the MIRC Nickname Buffer Overflow vulnerability.
February 3, 2002	**Safemodexploit.php**	**Exploit for the PHP MySQL Safe_Mode Filesystem Circumvention vulnerability.**
February 2, 2002	Sqlinjectionwhitepaper.pdf	A technique for exploiting web applications that uses client-supplied data in SQL queries without stripping illegal characters first.
January 30, 2002	**Crashme.java**	**Exploit for the Sun JRE Denial of Service vulnerability.**
January 30, 2002	Nbtenum11.zip	A utility for Windows which can be used to enumerate one single host or an entire class C subnet. This utility can run in two modes, query and attack.
January 30, 2002	**Netgear.txt**	**Perl script which exploits the NetGear RO318 HTTP Filter vulnerability.**
January 30, 2002	**Ntfs-hide.bat**	**Exploit for the Microsoft Windows NTFS File Hiding vulnerability.**
January 29, 2002	**Acedirector_request**	**Exploit for the AceDirector Half-Closed Session vulnerability.**
January 26, 2002	Kernel.keylogger.txt	Paper that describes the basic concepts and techniques used for recording keystroke activity under Linux. Also includes proof of concept.
January 26, 2002	**Symace.c**	**Script which exploits the BRU Insecure Temporary File vulnerability.**
January 24, 2002	**CA-2002-02.aol.icq**	**Exploit for the ICQ Buffer Overflow vulnerability.**

Trends

- **The National Infrastructure Protection Center (NIPC) has received reporting that infrastructure related information, available on the Internet, is being accessed from sites around the world. While in and of itself this information is not significant, it highlights a potential vulnerability. For more information, see NIPC ADVISORY 02-001, located at: http://www.nipc.gov/warnings/advisories/2002/02-001.htm.**
- **The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in CA-2001-31 and discussed in VU#172583. For more information, see CERT® Advisory CA-2002-01, located at: http://www.cert.org/advisories/CA-2002-01.html.**
- **NIPC has updated their advisory, NIPC Advisory 01-030, regarding what Microsoft refers to as a critical vulnerability in the universal plug and play (UPnP) service in Windows. For more information see, NIPC ADVISORY 01-030.3, located at: www.nipc.gov/warnings/advisories/2001/01-030-2.htm.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

IRC/Girls.worm (Internet Worm): This is a worm that spreads via IRC. Once received, user intervention is required to propagate the worm from your machine. Two files are appended to the end of the worm (compressed) - GIRLS(1).JPG and README.TXT. When the worm is executed as GIRLS.ZIP, these two files will be accessible to the user (assuming the ZIP extension is associated with ZIP archives).
The JPEG image is a pornographic photo. If the ZIP file extension is renamed to EXE, and then executed, the worm's propagation routine is run. The worm copies itself to %WINDIR%\GIRLS.ZIP. A countdown is displayed on the screen followed by a message box. The worm searches for MIRC.INI and PIRCH98.INI in the following folders on drives C, D, and E:

- MIRC.INI - \mirc\, \mirc32\, \progra~1\mirc\, and \progra~1\mirc32\
- PIRCH98.INI - \pirch98\ and \progra~1\pirch98\

If found, the worm drops the file SCRIPT.INI into that folder (overwriting any existing files of the same name). This file contains a single instruction to send a copy of the worm (%WINDIR%\GIRLS.ZIP) via IRC.

PE_GOSUSUB.A (Aliases: Gosusub.A, W32.HLLP.Gosusub) (File Infector Virus): This virus drops a copy of itself as WIN386.EXE in the Windows folder. Upon execution, it drops the file WIN386.EXE in the /%Windows%/ folder which is a copy of the virus. It modifies the system file SYSTEM.INI and the registry to allow this copy to execute. It modifies the SYSTEM.INI by changing a line in the [boot] section from:

Shell Explorer.exe
to
Shell Explorer.exe Win386.exe

It adds the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"Win386" "C:\Windows\Win386.exe"

This virus is also capable of infecting certain EXE files. Upon execution of its code, it searches the system for all drives, including the system mapped drives. It then searches for certain .EXE files in the directory:

- C:\Windows\Winrep.exe
- C:\Windows\System\!E4uinit.exe
- C:\Windows\System\Tapiini.exe
- C:\Windows\Command\Scanreg.exe

It infects the .EXE files by prepending its code to the file and then deletes .TXT files found in /%root%/, /%windows%/, /%system%/, and the following directories:

- C:\Windows\Command
- C:\Windows\Help.

W32/Klez-G (Win32 Worm): This is a Win32 worm that carries a compressed copy of the W32/ElKern-B virus, which it drops and executes when the worm is run. This worm searches for e-mail address entries in the Windows address book but uses it's own mailing routine. The e-mail subject is either random or chosen from a list. The worm randomly composes the message text but the message can also be without a text. An attached file is also included with randomly chosen names with extensions PIF, .SCR, .EXE, or .BAT. The sender address, which appears in a message, is chosen from a list inside the virus. W32/Klez-G attempts to disable several anti-virus products and delete some anti-virus related files. The worm attempts to exploit a MIME vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double-clicking on the

attachment. Microsoft has issued a patch that secures against this vulnerability that can be downloaded from http://www.microsoft.com/technet/security/bulletin/MS01-027.asp. *(Note: This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this worm.)* The virus may also spread to remote shares on other machines using random filenames. It copies itself to the Windows System directory with a random filename. The worm will set the registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

to point to the worm file, so that the file is run on Windows startup.

W32/Tariprox-B (Win32 Worm): This is a proxy worm that attaches itself to out-going e-mail messages. The worm will arrive as an e-mail attachment called <username>.doc.pif, where <username> is the name of the e-mail recipient. When run, it copies itself to the Windows directory as MMOPLIB.EXE and creates the registry entry:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\mmoplib = Windows>\MMOPLIB.EXE,

so that the worm is run automatically each time the machine is restarted. It also replaces/creates the HOSTS file, which maps machine names to IP addresses. Various network-related programs, such as Outlook and Outlook Express use the HOSTS file, in order to quickly resolve machine IP addresses (rather than having to query the DNS database). In order to work on both Win9x and NT machines, the worm will try to create or replace the file HOSTS or HOSTS.bak in the Windows and Winnt\System32\drivers\etc\ directories. The existing HOSTS file may be named HOSTS.sam (the default for W95/W98) in which case it will remain unchanged. However, the version created by the worm (without an extension) will be used. The worm creates an entry in the new HOSTS file, which maps the default SMTP server to the loop-back address 127.0.0.1. The worm then runs in the background waiting to accept a connection on port 25 (the SMTP port). When the user tries to send an e-mail, the e-mail client program (such as Outlook or Outlook Express) tries to establish a connection to the SMTP server on port 25, but mistakenly uses the address 127.0.0.1 and so actually connects to the worm. The worm establishes a connection to the real SMTP server (on port 25) and acts as a go-between, sending its own data at the appropriate moment. The worm avoids repeatedly sending itself to the same person by keeping a list of the five most recent recipients in the following registry key:

HKLM\Software\Microsoft\Media Optimization library\MRU = NULL, NULL, recipient3, recipient2, recipient1.

It does not attach itself to e-mail messages destined for these people. On some networks, the same machine acts as both the outgoing and incoming mail server. If this is the case, when an e-mail client attempts to connect to the server to download e-mail, the worm accepts the connection but doesn't pass on responses if they're not related to sending e-mail. This may prevent the user from downloading new e-mails. Any other programs that use the HOSTS file to resolve IP addresses (such as Telnet) will also be unable to establish a connection to the machine acting as the default SMTP server, because they will attempt to connect to 127.0.0.1. On many network configurations however, there will be one machine to handle SMTP and one to handle POP3 (or IMAP, DSMP etc.). On these networks the worm will function as intended. The worm was designed primarily to work with Outlook Express and so may not work properly with other MAPI client programs. W32/Tariprox-B is a Windows PE executable. UPX packed versions also exist. The worm contains the text: 'W32.Taricone-B.worm@proxy by I.V.E.L.'

WM97/Comical-A (Word 97 Macro Worm): This is a mass mailing e-mail worm. It consists of three components: a Word macro file, a Visual Basic script and a Windows executable. These three components are detected as WM97/Comical-A, VBS/Comical-A and W32/Comical-A respectively. WM97/Comical-A arrives in an e-mail with the following characteristics:

Subject line: A comical story for you
Message text: I send you a comical story found on the Net.
Best Regards, You friend.
Attached file: comical_story.doc

When the attachment is launched using Microsoft Word, it will display a dialog box that states 'This file has some problems.' When the user clicks on the OK box, the worm will drop a Visual Basic script, VBS/Comical-A, to C:\twin.vbs. The worm will then execute VBS/Comical-A. VBS/Comical-A will collect e-mail addresses from the Outlook address book and write them to the file C:\backup.win. It will create the Word document Netinfo.doc in the Windows directory. This file is detected as

WM97/Comical-A. It will then write avw32.exe into the Windows directory and execute it. The virus will attempt to send Netinfo.doc to all the e-mail addresses listed in C:\backup.win. It will also add the following registry key to ensure that the executable is run on startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\AntiVirus Freeware

The executable will also delete the file C:\twin.vbs.

W32/MyParty-A (Aliases: W32/Myparty@mm, W32.Myparty@mm) (Win32 Worm): This virus has been reported in the wild. It is a Windows 32 e-mail-aware worm which arrives as an e-mail message with the subject "new photos from my party!" and an attachment, www.myparty.yahoo.com. Some people may be fooled into believing the attached file is a link to a website. If the attached file is executed, the worm sends a copy of itself to everybody in the Windows Address book (except the current user) using a built in SMTP engine. It gets the SMTP server information from the registry key:

HKCU\Software\Microsoft\Internet Account Manager\Accounts\00000001

The worm also sends an e-mail to napster@gala.net to track its spread.

W32.Myparty.B@mm (Aliases: WORM_MYPARTY.B, MYPARTY.B) (Win32 Worm): This variant of WORM_MYPARTY.A also arrives in an e-mail with the subject line "new photos from my party!" but includes the attachment "myparty.photos.yahoo.com." Similar to WORM_MYPARTY.A, this variant copies itself to C:\Recycled\REGCTRL.EXE in Windows 9x. In Windows NT it copies itself to C:\REGCTRL.EXE and drops a file named msstask.exe in "%windows%\profile\%username%\ Start Menu\Programs\Startup." It also drops the following file that is only visible in MS-DOS prompt:

C:\RECYCLER\F-&ltRandom Number>-&ltRandom Number>-&ltRandom Number> (This is the actual file)

or

C:\RECYCLED\F-&ltRandom Number>-&ltRandom Number>-&ltRandom Number>> (This is the actual file)

However, between the system dates of January 20–24, 2002 this file with a random filename will not be dropped at C:\RECYCLER nor at C:\RECYCLED. This is different from the trigger date of WORM_MYPARTY.A that is January 25–29, 2002. It also sends an infected e-mail with the same message and subject used by WORM_MYPARTY.A but with a different file attachment name.

W32.Rexli.A@mm (Win32 Worm): This is a mass-mailing worm that is written in Visual Basic. When executed, the worm e-mails all contacts in the Microsoft Outlook address book. If mIRC is found, the worm modifies a file called Script.ini. This modification causes an infected user to send the worm to people over the IRC network.

W32.Sysnom.C@mm (Win32 Worm): This is a mass-mailing worm that copies itself to C:\Windows \SoftwareKey.exe. When it is executed, it sends itself to all contacts in the Microsoft Outlook address book. When the AVP button is clicked, it opens Internet Explorer to the Web site http:/ /www.avp.ch. It will also ping the site ndovirus.8m.com. Finally, the worm copies itself to C:\Windows\SoftwareKey.exe.

W97M.DebilByte.A (Word 97 Macro Virus): This is a simple macro virus that resides in eight macro modules. Each module is exported to the files Wdr1.sys, Wdr2.sys, . . . Wdr8.sys, which are created in the Windows directory. The module files are then used by the virus to infect the Normal.dot template file as well as any other document whenever a document is opened or closed. The virus also disables the following menu commands:

- Tools > Macro > Macros... (Alt+F8)
- Tools > Macro > Visual Basic Editor (Alt+F11)

The only text string in the virus is a URL pointing to the Russian Yandex site.

W97M_NOMED.A (Aliases: Macro.Word97.Demo.C, NOMED.A): This macro virus infects Word 97 documents. It copies its viral codes to a "DEMON" module in infected documents. It does not have a destructive payload.

WM97/Falcon-A (Word 97 Macro Virus): This virus replicates with errors. On an infected system, access to the File|Templates and the Visual Basic Editor is disabled. When a user attempts to access the VB Editor, two message boxes are displayed: One has the title "CVBEditor::ShowWindow() error!" and contains the text "Installation error 0x80000025 Please reinstall Visual Basic for Applications."
The other displayed message box has the title "MacroProt v2.0 Beta" with the text "To prevent viruses the system administrator has disabled Macro editing."

WORM_COUPLE.A (Aliases: COUPLE.A, VBS_COUPLE.A, VBS_LASTSCENE.B, WORM_LASTSCENE) (Worm): This mass-mailing worm propagates via e-mail using MAPI and Microsoft Outlook, and installs backdoor programs on the infected user's computer. The e-mail arrives with the subject line: "Nice Couple."

WORM_HUNCH.A (Aliases: HUNCH.A, W32.Hunch@mm) (Worm): This memory-resident worm propagates via Microsoft Outlook by sending copies of itself to all addresses listed in the infected user's address book. It arrives as an attachment called "COSTOS DE PRODUCCION.xls.exe." It modifies the registry to allow it to execute at every Windows startup.

WORM_NAVIDAD.A (Aliases: NAVIDAD, TROJ_NAVIDAD.A, W32/Navidad@M, W32.Navidad) (Internet Worm): This Internet worm propagates via Microsoft Messaging API (MAPI). It responds to messages included in the user INBOX using the default MAPI client and e-mail. Every response has the subject, "RE:" and the worm as an attachment (NAVIDAD.EXE). This worm also displays a message box upon execution and maps the opening of Windows executables so that it is executed instead of the executable that is called.

WORM_PORMAN.A (Aliases: I-Worm.Alcaul.m, W32.Porma@mm, PORMAN.A) (Worm): This mass-mailing worm sends an infected e-mail via Microsoft Outlook with the attachment http.www.sex.com, and the subject line "pornoman recommends."

WORM_WHITEBAIT.A (Aliases: WHITEBAIT.A, W32.Whitebait@mm) (Worm): This mass-mailing worm propagates via Microsoft Outlook and arrives in an e-mail with the subject line attachment "WARNING : Black_Piranha" and the attachment "MSSECU.EXE." Upon execution, it drops two files in the Windows folder, and displays pornographic pictures with a link to an adult-oriented Web site.

XM97/Divi-AQ (Excel 97 Macro Virus): This virus is a member of the XM97/Divi family with no malicious payload. It creates the viral file 874.xls in the XLSTART directory.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	**N/A**	**Current Issue**
Backdoor.Palukka	N/A	CyberNotes-2002-01
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-FB.svr.gen	**N/A**	**Current Issue**
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	**N/A**	**Current Issue**
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
SecHole.Trojan	N/A	CyberNotes-2002-01
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/Msstake-A	**N/A**	**Current Issue**
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	**N/A**	**Current Issue**
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	**N/A**	**Current Issue**
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS_THEGAME.A	**N/A**	**Current Issue**

APStrojan.sl: This Trojan attempts to steal AOL Instant Messenger usernames and passwords. It also logs keystrokes and sends this data to a Yahoo.com e-mail address. When run, the Trojan copies itself to the WINDOWS\START MENU|PROGRAMS\STARTUP folder. If AOL Instant Messenger is not installed, an error message appears. All window titles and keystrokes typed are logged to the file DAT.LOG in the same directory as the executable (the STARTUP folder). With this information, the Trojan attempts to create the file C:\PROGRAM FILES\DMSYSMAIL.EML and send it, using MAPI messaging to it090d@yahoo.com.

BackDoor-FB.svr.gen: This Trojan is dropped by the W32/Myparty@mm virus. When the W32/Myparty@MM virus executable is executed on Windows NT machines, (Windows NT, 2000 or XP) a variant of this backdoor is dropped to the startup folder within the profile of the current user, MSSTASK.EXE:

%userprofile%\Start Menu\Programs\Startup\msstask.exe

This ensures the backdoor is executed upon system startup, at which point it goes memory resident, and the machine is becomes vulnerable. W32/Myparty@MM only massmails itself and drops the backdoor component if the system date is within the following range: 25th - 29th January 2002, inclusive. Outside of this date range, no backdoor component is dropped. MSSTASK.EXE is compressed with UPX. Once running, the backdoor tries to connect to the following IP address: http://209.151.250.170/, in order to download the command file that operates the backdoor. A second W32/Myparty@MM variant, which only operates between 20th-24th January 2002, drops an identical backdoor component to that described above. The only difference is the date range in which the backdoor is dropped.

DoS-Winlock: This Trojan initiates a Denial of Service attack against several systems, most of which are in the langame.net domain. The executable has been packed with the PECompact packer. When run, the Trojan copies itself to WINDOWS directory as NETDLL16.EXE and the Recycle Bin as Winlock.exe with hidden file attributes. A WIN.INI entry is added to load itself at startup, run=C:\RECYCLED\winlock.exe. The next time Windows is rebooted, the Trojan starts its DoS attack and stays resident in memory.

Irc-Smallfeg: Users are most likely to encounter this Trojan in the form of a dropper (which may be named ModemSpeedEnhancer.Exe). When executed on NT/2000 the dropper creates the folder, %WINDIR%\CACHE, and drops the file SVCHOST.EXE into it. Subsequently, SVCHOST.EXE is executed as a process. When executed on Windows 9x machines, the dropper is harmless - it does not drop the server component. Once running as a process, the file JUPE.DLL is dropped in the %WINDIR%\CACHE directory. This file contains a small amount of encrypted data,(possibly information about the victim machine). The Trojan then attempts to connect to port 6667 of 22 various remote servers (all -----.--.undernet.org). If successful, the Trojan then attempts to join a specific channel in the Undernet IRC network, with a nickname built up from two words stored within the SVCHOST.EXE file (e.g. gold, plat, fat, bomb, hehe, goal).

TROJ_DSNX.A (Aliases: DSNX, DSNX.A, Trojan.Win32.DSNX): This destructive Win32 Trojan enables a remote malicious user access to an infected computer. It compromises network security. Upon execution, this Trojan copies itself to a WIN<text>.EXE file in the Windows System directory, where <text> is a randomly generated text string. It then adds the following registry entry that allows it to run at every startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run = WinDSNX

The Trojan then connects to an IRC server and joins a channel where the remote malicious user is connected. The remote malicious user may execute any or all of the following in an infected system:

- Upload/Download files
- Perform a port scan on the local area network
- Flood a specified IP address
- Log keystrokes
- Delete files

TROJ_ICONLIB.A (Aliases: Trojan.IconLib, ICONLIB.A, ICONLIB): This Trojan's destructive payload deletes system files on the infected computer. It then replaces deleted files with copies of itself. Thereafter, the infected system hangs, due to missing system files, and will no longer restart.

Troj/Msstake-A (Alias: BackDoor-AAF): This is a backdoor Trojan that allows others to have remote access to your machine over a network. It is dropped by the W32/MyParty-A virus.

VBS_THEGAME.A (Alias: THEGAME.A): This Script Trojan has the ability to mass mail, drop other Trojan files, modify registries, and modify WIN.INI. It is encrypted but not destructive.